

10/554215

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP05/052530

International filing date: 02 June 2005 (02.06.2005)

Document type: Certified copy of priority document

Document details: Country/Office: DE
Number: 10 2004 037 801.0
Filing date: 03 August 2004 (03.08.2004)

Date of receipt at the International Bureau: 22 July 2005 (22.07.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

BEST AVAILABLE COPY



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

BEST AVAILABLE COPY

BUNDESREPUBLIK DEUTSCHLAND



05.07.2005

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

CERTIFIED COPY OF PRIORITY DOCUMENT

Aktenzeichen: 10 2004 037 801.0

Anmeldetag: 03. August 2004

Anmelder/Inhaber: Siemens Aktiengesellschaft, 80333 München/DE

Bezeichnung: Verfahren zur sicheren Datenübertragung

IPC: H 04 L, G 07 C

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 28. Juni 2005
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Weber

Wenner

Beschreibung

Verfahren zur sicheren Datenübertragung

5 Die Erfindung betrifft ein Verfahren zur sicheren Datenübertragung zwischen einem ersten Teilnehmer und zweiten Teilnehmern, insbesondere einem Fahrtschreiber eines Nutzfahrzeuges und Speicherkarten mit jeweils mindestens einem Datenspeicher, wobei der erste Teilnehmer einen Speicher aufweist, in
10 welchem eine bestimmte Anzahl Einträge gespeichert sind, jeweils umfassend Kennungen und zu diesem zugeordnete Sicherheitszertifikate zweiter Teilnehmer mit einer Erfassungszeit des Sicherheitszertifikates.

15 Verfahren zur sicheren Datenübertragung gewinnen zunehmend an Bedeutung und existieren bereits in umfassender Vielfalt im Bereich von Computernetzwerken. Im weiteren Sinne vergleichbar mit modernen Computernetzwerken ist auch das Zusammenwirken bzw. die sichere Datenübertragung eines digitalen Fahrt-
20 schreibers mit einer Speicherkarte gemäß der EG-Verordnung 3821/85. Zur Gewährleistung der Einhaltung bestehender Sozialvorschriften und Gesetze am Arbeitsplatz des Nutzfahrzeuges ist die Erhöhung der Manipulationssicherheit von besonderer Bedeutung. Daher werden strengste Maßstäbe an die Sicherheit
25 der Datenübertragung gelegt. Hierzu ist ein System von Sicherheitszertifikaten umfassend verschiedene öffentliche und private Schlüssel entwickelt worden, welches im Einzelnen der vorgenannten Verordnung entnehmbar ist. Bevor ein erster Teilnehmer bzw. der Fahrtschreiber mit einem zweiten Teilnehmer bzw. einer Speicherkarte in einen Datenaustausch eintreten kann, ist unter anderem ein sehr aufwendiges Verfahren der Sicherheitszertifikatsverifikation auf beiden Seiten der Teilnehmerschaft erforderlich. Der Umfang dieses Vorgangs und

die eingeschränkten Möglichkeiten der Datenverarbeitung in dem kleinformatigen Gerät machen besondere Vorkehrungen erforderlich, damit die Zugriffszeiten bei akzeptablem Kostenaufwand in einem vernünftigen Rahmen bleiben.

5

Daher hat es sich die Erfindung zur Aufgabe gemacht, den insbesondere zeitlichen Aufwand der Sicherheitszertifikatsverifikationen für die Teilnehmer des Datenaustauschs ohne Einbußen der Manipulationssicherheit zu reduzieren.

10

Zur Lösung der Aufgabe wird erfindungsgemäß ein Verfahren der eingangs genannten Art vorgeschlagen, bei welchem vorgesehen ist, dass der erste Teilnehmer von dem zweiten Teilnehmer eine Kennung einholt, der erste Teilnehmer diese Kennung mit

15 den in dem Speicher gespeicherten Kennungen vergleicht, wenn eine übereinstimmende Kennung in dem Speicher gespeichert ist, dass dieser Kennung zugeordnete Sicherheitszertifikat Basis für eine nachfolgende Datenübertragung ist und die Erfassungszeit des Sicherheitszertifikates auf eine aktuelle

20 Systemzeit aktualisiert wird, wenn keine übereinstimmende Kennung in dem Speicher gespeichert ist, der erste Teilnehmer eine Sicherheitszertifikatsverifikation mit dem zweiten Teilnehmer durchführt und bei Verifizierung einen dem verifizierten Sicherheitszertifikat entsprechenden Eintrag mit aktuel-

25 ler Erfassungszeit in dem Speicher speichert, wobei der Eintrag mit dem ältesten Erfassungsdatum durch diesen neuen Eintrag ersetzt wird, wenn die bestimmte Anzahl an Einträgen schon erreicht war.

30 Ein entscheidender Vorteil des erfindungsgemäßen Verfahrens liegt in der Einsparung des sehr zeitaufwendigen Vorganges der Sicherheitszertifikatsverifikation für den Fall, dass dem ersten Teilnehmer der zweite Teilnehmer auf Grund eines in

der Vergangenheit bereits durchgeführten Verifikationsvorgänge bekannt ist. Aus Speicherplatzgründen, insbesondere bei der Ausbildung des ersten Teilnehmers als Fahrtschreiber und des zweiten Teilnehmers als Speicherkarte, ist eine Begrenzung der Anzahl der Einträge umfassend die Sicherheitszertifikate und die Erfassungszeit der Sicherheitszertifikate anderer Teilnehmer begrenzt. Um trotz dieser Begrenzung das "Erinnerungsvermögen" des ersten Teilnehmers an zweite Teilnehmer auf eine Höchstanzahl an zweiten Teilnehmern zu optimieren, sieht das erfindungsgemäße Verfahren nicht eine einfache Ringspeicherung in chronologischer Abfolge des Auftretens der zweiten Teilnehmer vor, so dass stets beispielsweise der älteste Eintrag mit dem neuesten Eintrag überschrieben wird, wenn eine speicherplatzbedingte Höchstzahl an Einträgen schon erreicht war. Statt dessen wird zunächst der Inhalt des Speichers des ersten Teilnehmers daraufhin überprüft, ob bereits ein Eintrag mit identischer Kennung zu derjenigen des neuen Teilnehmers existiert, der im bejahenden Fall lediglich hinsichtlich des Erfassungsdatums und gegebenenfalls hinsichtlich des Ablaufs der Gültigkeit des Sicherheitszertifikates aktualisiert wird. Auf diese Weise sind dem ersten Teilnehmer, vorausgesetzt es wurde in der Vergangenheit bereits eine die bestimmte Anzahl an Speichereinträgen übersteigende Anzahl unterschiedlicher zweiter Teilnehmer verifiziert, stets die bestimmten Anzahl an zweiten Teilnehmern bekannt. Auf diese Weise kann die bestimmte Anzahl entsprechend den Gepflogenheiten beispielsweise eines Fuhrparks an die Anzahl der dort tätigen oder üblicherweise mit dem Nutzfahrzeug arbeitenden unterschiedlichen Karteninhaber angepasst werden und so eine optimale Nutzung des Speichers des ersten Teilnehmers erreicht werden. Die Zugriffszeiten bleiben vorteilhaft kurz, da auch bei wiederholtem Trennen und Verbinden des ersten Teilnehmers und des zweiten Teilnehmers stets nur die

der Identität des ersten Teilnehmers zugeordneten Einträge verändert bzw. aktualisiert werden.

Mit Vorteil ist die zur Identifizierung übermittelte Kennung
5 der Teilnehmer ein öffentlicher Schlüssel eines RSA-Verfah-
rens (Verfahren zum Ver- und Entschlüsseln nach Ronald L. Ri-
vest, Adi Shamir und Leonard Adleman) des zweiten Teilneh-
mers ist. Dieser öffentliche Schlüssel kann einerseits einer
nachträglichen Datenübermittlung dienen und ist andererseits
10 eindeutig.

Aus Gründen der Ersparnis von Rechenaufwand sieht eine vor-
teilhafte Weiterbildung vor, dass eine nachfolgende Daten-
übertragung mittels einer symmetrischen Verschlüsselung, ins-
15 besondere eines Triple-DES-Verfahrens erfolgt, wobei nach er-
folgter Verifizierung der Sicherheitszertifikate beide Teil-
nehmer eine Zufallszahl verschlüsselt an den anderen Teilneh-
mer übersenden und beide Teilnehmer jeweils unabhängig von-
einander mittels der beiden Zufallszahlen einen gemeinsamen
20 Schlüssel zur Datenübertragung unter Benutzung desselben Al-
gorithmus bestimmen. Im Wesentlichen bleibt hierbei die Si-
cherheit des asymmetrischen Verschlüsselungsverfahrens erhal-
ten, da die Generierung des Sitzungsschlüssels für das sym-
metrische Verfahren nur demjenigen möglich ist, der zuvor
25 mittels des asymmetrischen Verfahrens in der Lage war, mit
dem anderen Teilnehmer zu kommunizieren bzw. die wechselsei-
tig übermittelte Zufallszahl zu dechiffrieren.

Eine wichtige Position hinsichtlich der Manipulationssicher-
heit übernimmt gemäß dem Verfahren nach der Erfindung die Ve-
rifikation der Sicherheitszertifikate durch den jeweils ande-
ren Teilnehmer, weshalb diese zweckmäßig folgende n Schritte
umfasst:

In einem ersten Schritt übersendet der zweite Teilnehmer dem ersten Teilnehmer ein erstes Sicherheitszertifikat, welches der zweite Teilnehmer unter Benutzung eines ersten öffentlichen Schlüssels einer Verifizierung unterzieht und hierbei 5 einen zweiten öffentlichen Schlüssel ermittelt. Resultiert die Verifizierung in Authentizität des übermittelten Sicherheitszertifikates, wird der erste Schritt unter Verwendung eines weiteren übersendeten Sicherheitszertifikates und des im vorhergehenden Schritt ermittelten zweiten öffentlichen 10 Schlüssels anstelle des ersten öffentlichen Schlüssels (n-1)-fach wiederholt, wobei sich stets ein neuer zweiter öffentlicher Schlüssel und ein Verifizierungsergebnis ergibt. Diese verschachtelte Verifizierung kann zweckmäßig 3(=n)-fach wiederholt werden, was eine sehr hohe Manipulationssicherheit 15 zum Ergebnis hat.

In der Folge ist die Erfindung anhand eines speziellen Ausführungsbeispiels unter Bezugnahme auf Zeichnungen zur Verdeutlichung näher beschrieben. Es zeigen:

20

Figur 1 eine schematische Darstellung des erfindungsgemäßen Verfahrens in Form eines Flussdiagramms,

25

Figur 2 ein Flussdiagramm des Vorgangs der Sicherheitszertifikatsverifizierung,

Figur 3 Einträge bekannter zweiter Teilnehmer in einem Speicher eines ersten Teilnehmers.

30

Das Flussdiagramm der Figur 1 zeigt beispielhaft wesentliche Züge des Ablaufes eines erfindungsgemäßen Verfahrens an einem Datenaustausch zwischen einem digitalen Fahrtschreiber 51 und einer Speicherkarte 50.

Das einleitende Ereignis 1 besteht in der Aufnahme 2 der Speicherkarte 50 mittels des Fahrtschreibers 51. Im Rahmen der Aufnahme 2 der Speicherkarte 50, welche im erfindungsgemäßen Sinne ein zweiter Teilnehmer T2 ist, stellt der Fahrt-
5 schreiber, welcher im erfindungsgemäßen Sinne ein erster Teilnehmer T1 ist, eine leitende Verbindung zu einem Datenspeicher der Speicherkarte 50 her, mittels derer Datensignale übertragbar sind.

10 In einem zweiten Schritt 3 holt der Fahrtschreiber 51 als erster Teilnehmer T1 von der Speicherkarte 50 als zweiten Teilnehmer T2 eine Kennung 4 ein und überprüft in einem dritten Schritt 5, ob die Kennung 4 bereits aus einem vorhergehenden Vorgang bekannt ist. Hierzu greift der Fahrtschreiber 51 auf einen integrierten Speicher 6 zu, in welchem Einträge mit in Figur 3 näher beschriebenem Umfang abgelegt sind.

Ist im Speicher 6 kein mit der Kennung 4 der Speicherkarte 50
20 abgelegter Eintrag vorhanden, geht das erfindungsgemäße Verfahren zu einer wechselseitigen Sicherheitszertifikatsverifikation 7 über. Hierbei werden während einer ersten Sicherheitszertifikatsverifikation Sicherheitszertifikate der Speicherkarte 50 mittels des Fahrtschreibers auf Gültigkeit, Be-
25 kantheit und Authentizität gemäß Figur 2 überprüft, und anschließend findet eine entsprechende zweite Überprüfung 9 des Fahrtschreibers 51 seitens der Speicherkarte 50 statt.

Die Schritte 8 und 9 werden übersprungen, wenn im Schritt 5
30 der zweite Teilnehmer T2 bzw. die Speicherkarte 50 seitens des ersten Teilnehmers T1 als bekannt identifiziert wurde. Ist das endgültige Ergebnis einer Sicherheitszertifikatsverifikation gemäß der Schritte 8, 9 die Nicht-Verifikation, wird

die Speicherkarte 50 bzw. der erste Teilnehmer T1 in einem Schritt 10 ausgegeben bzw. abgewiesen.

Bei erfolgreicher wechselseitiger Verifikation bzw. bekannter 5 Kennung 4 folgt in einem Schritt 11 ein wechselseitiger Austausch einer Zufallszahl in RSA-verschlüsselter Form, mittels derer in einem Schritt 12 ein gemeinsamer Sitzungsschlüssel 60 von beiden Teilnehmern T1, T2 unabhängig generiert wird, der im nachfolgenden Schritt 13 der symmetrischen Ver- 10 schlüsselung übertragener Daten dient.

In Figur 2 ist die Sicherheitszertifikatsverifikation gemäß der Schritte 8, 9 in Figur 1 im Detail dargestellt. In einem ersten Schritt 21 holt der zweite Teilnehmer T2 von dem ersten Teilnehmer T1 ein Sicherheitszertifikat Cert.Lev.1 der ersten Ebene ein. Anhand von Einträgen eines Speichers 22 wird in einem zweiten Schritt 23 überprüft, ob der öffentliche Schlüssel oder eine Kennung des Sicherheitszertifikats Cert.Lev.1 der ersten Ebene bereits bekannt und noch gültig 15 ist. Für den Fall der Gültigkeit und Bekanntheit geht das dargestellte Verfahren direkt zu einem Schritt 24 über, währenddessen der erste Teilnehmer T1 das Sicherheitszertifikat des zweiten Teilnehmers T2 in gleicher, nicht mehr gesondert dargestellter Weise einer Überprüfung unterzieht. Ist der öffentliche Schlüssel des Sicherheitszertifikats Cert.Lev.1 der Ebene 1 in dem Schritt 23 als nicht bekannt identifiziert 20 worden, holt der zweite Teilnehmer T2 von dem ersten Teilnehmer T1 ein Sicherheitszertifikat Cert.Lev.2 der Ebene 2 in einem nachfolgenden Schritt 25 ein. Entsprechend dem Schritt 25 25 folgt in analoger Weise ein Schritt 26, währenddessen der zweite Teilnehmer T2 unter Zugriff auf den Speicher 22 die Bekanntheit und Gültigkeit eines öffentlichen Schlüssels des Sicherheitszertifikats Cert.Lev.2 der Ebene 2 überprüft. Ist 30

das Ergebnis der Überprüfung Bestätigung der Bekanntheit und Gültigkeit, geht das Verfahren direkt zu einem Verifizierungsschritt 27 über, währenddessen das Sicherheitszertifikat Cert. Lev.1 Ebene 1 einer Verifizierung unterzogen wird.

5 Ist der öffentliche Schlüssel des Sicherheitszertifikats Cert. Lev.2 der Ebene 2 nicht bekannt und gültig, folgt zunächst die Verifizierung des Sicherheitszertifikats Cert. Lev.2 der Ebene 2 in einem Schritt 28, bevor die Verifizierung gemäß Schritt 27 eingeleitet wird. Haben die Überprüfungen der Schritte 27 und 28 Verifizierung der Sicherheitszertifikate Cert. Lev.1,2 der Ebene 1 und Ebene 2 zum Ergebnis, geht das Verfahren zum Schritt 24 über, welches eine bezüglich der Teilnehmer T1 und T2 umgekehrte Sicherheitszertifikatsverifikation einleitet.

15 Die Figur 3 zeigt den Inhalt des Speichers 22 bzw. 6 in Abhängigkeit eines Kommunikationseintrittes verschiedener zweiter Teilnehmer T2 mit einem ersten Teilnehmer T1. Die Größe des Speichers 6, 22 ist auf fünf Einträge 31-35 begrenzt. Es sind sechs aufeinander folgende Zustände 41-46 in Figur 3 abgebildet, die jeweils die Einträge 31-34 nach bestimmten Ereignissen wiedergeben. Die dargestellten Einträge 31-34 umfassen ein Datum 51, dessen Wert in hexadezimaler Schreibweise als Wert in Sekunden seit dem 1.1.1970 abgelegt ist. Daneben umfassen die Einträge 31-35 einen Sicherheitszertifikatsinhalt 52, der einen Ablauf EOV der Gültigkeit des Sicherheitszertifikats und eine Referenz CHR des Sicherheitszertifikatinhabers umfasst. Daneben umfassen die Einträge 31-35 auch die Erfassungszeit 53.

20 25 30 Der Zustand 41 zeigt den Ausgangszustand, der charakterisiert ist durch neutrale Einträge.

Der Zustand 42 liegt vor, nachdem fünf verschiedene zweite Teilnehmer T2 bzw. Speicherkarten 50 mit dem Teilnehmer T1 bzw. einem Fahrtenschreiber 51 in datenübertragenden Kontakt getreten sind. Demzufolge ist jeder Eintrag 31-35 nun gekenn-
5 zeichnet durch ein anderes Datum, einen unterschiedlichen Sicherheitszertifikatsinhalt 52 und eine andere Erfassungszeit 53.

Der Zustand 43 stellt sich ein, nachdem ein zweiter Teilnehmer 10 ursprünglich charakterisiert durch den Eintrag 33 zu einem späteren Zeitpunkt nochmals mit dem ersten Teilnehmer T1 in einen datenübertragenden Kontakt getreten ist. Demzufolge hat sich die Erfassungszeit 53 des Eintrages 33 aktualisiert.

15 Der Zustand 44 stellt sich ein, wenn bereits eine der Obergrenze an Einträgen 31-35 entsprechende Anzahl jeweils auf Grund einer Verbindung mit einem zweiten Teilnehmer T2 de-neutralisiert worden sind und ein weiterer, bisher noch nicht bekannter zweiter Teilnehmer T2 mit dem ersten Teilnehmer T1
20 in einen datenübertragenden Kontakt tritt. Der gemäß der Erfassungszeit 53 älteste Eintrag 31 ist erfindungsgemäß mit einem neuen Eintrag 36 überschrieben.

In analoger Weise wird der Eintrag 32 in Zustand 45 von einem
25 Eintrag 37 ersetzt.

Zustand 46 stellt sich ein, wenn ein mit dem ursprünglichen Eintrag 31 korrespondierender zweiter Teilnehmer T2 nochmals mit dem ersten Teilnehmer T1 eine datenübertragende Verbindung eingeht. Auch hier wird der nunmehr älteste Eintrag 34
30 von dem Eintrag 31, der einem in Folge des Überschreibs aus Zustand 44 unbekannten zweiten Teilnehmer T2 zugeordnet ist,
ersetzt.

Patentansprüche

1. Verfahren zur sicheren Datenübertragung zwischen einem ersten Teilnehmer (T1) und zweiten Teilnehmern (T2), insbesondere zwischen einem Fahrtschreiber (51) eines Nutzfahrzeugs und Speicherkarten (50) mit jeweils mindestens einem Datenspeicher, wobei der erste Teilnehmer (T1) einen Speicher (6, 22) aufweist, in welchem eine bestimmte Anzahl Einträge (31-35) gespeichert sind, jeweils umfassend Kennungen (4) und zu diesen zugeordnete Sicherheitszertifikate (Cert) zweiter Teilnehmer (T2) mit einer Erfassungszeit (53) des Sicherheitszertifikates (Cert),
5 welches Verfahren umfasst, dass der erste Teilnehmer (T1) von dem zweiten Teilnehmer (T2) eine Kennung (4) einholt, der erste Teilnehmer (T1) diese Kennung (4) mit den in dem Speicher (6, 22) gespeicherten Kennungen (4) vergleicht,
10 wenn eine übereinstimmende Kennung (4) in dem Speicher (6, 22) gespeichert ist, das dieser Kennung (4) zugeordnete Sicherheitszertifikat (Cert) Basis für eine
15 nachfolgende Datenübertragung ist und die Erfassungszeit (53) des Sicherheitszertifikates (Cert) auf eine aktuelle Systemzeit aktualisiert wird,
20 wenn keine übereinstimmende Kennung (4) in dem Speicher (6, 22) gespeichert ist, der erste Teilnehmer (T1) eine Sicherheitszertifikatsverifikation mit dem zweiten Teilnehmer (T2) durchführt und bei Verifizierung einen
25 dem verifizierten Sicherheitszertifikat (Cert) entsprechenden Eintrag (31-35) mit aktueller Erfassungszeit (53) in dem Speicher (6, 22) speichert, wobei der Eintrag (31-35)
30 mit dem ältesten Erfassungsdatum durch diesen neuen Eintrag (31-35) ersetzt wird, wenn die bestimmte Anzahl an Einträgen (31-35) schon erreicht war.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Kennung (4) ein öffentlicher Schlüssel eines RSA-Verfahrens des zweiten Teilnehmers (T2) ist.
- 5 3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine nachfolgende Datenübertragung TDES-verschlüsselt erfolgt, wobei nach erfolgter Verifizierung der Sicherheitszertifikate (Cert) beide Teilnehmer (T1, T2) eine Zufallszahl (RND) verschlüsselt an den anderen Teilnehmer (T1, T2) übersenden und beide Teilnehmer (T1, T2) jeweils unabhängig voneinander mittels der beiden Zufallszahlen (RND) einen gemeinsamen Schlüssel (80) zur Datenübertragung unter Benutzung des selben Algorithmus bestimmen.
- 15 4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Verifikation des Sicherheitszertifikats (Cert) des ersten Teilnehmers (T1) durch den zweiten Teilnehmer (T2) und umgekehrt folgende n Schritte umfasst:
 - 20 in einem ersten Schritt übersendet der zweite Teilnehmer (T2) dem ersten Teilnehmer (T1) ein erstes Sicherheitszertifikat (Cert.Lev.1), welches der zweite Teilnehmer (T2) unter Benutzung eines ersten öffentlichen Schlüssels einer Verifizierung unterzieht und hierbei einen zweiten öffentlichen Schlüssel ermittelt, resultiert die Verifizierung in Authentizität,
 - 25 wird der erste Schritt unter Verwendung eines weiteren übersendeten Sicherheitszertifikats (Cert.Lev.1,2) und des im vorhergehenden Schritt ermittelten zweiten öffentlichen Schlüssels an Stelle des ersten öffentlichen Schlüssels (n-1)-fach wiederholt, wobei sich stets ein

neuer zweiter öffentlicher Schlüssel und ein Verifizierungsergebnis ergibt.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass $n=3$ ist.

5

Zusammenfassung

Verfahren zur sicheren Datenübertragung

- 5 Die Erfindung betrifft ein Verfahren zur sicheren Datenübertragung, insbesondere zwischen einem Fahrtschreiber (51) eines Nutzfahrzeuges und Speicherkarten (50), wobei ein erster Teilnehmer (T1) einen Speicher (6, 22) mit Einträgen (31-35) umfassend Kennungen (4) und Sicherheitszertifikate (Cert)
- 10 zweiter Teilnehmer (T2) aufweist. Verfahren zur sicheren Datenübertragung gewinnen zunehmend an Bedeutung und gehen häufig mit hohem Rechenaufwand einher. Daher hat es sich die Erfindung zur Aufgabe gemacht, die Rechenzeit hierfür ohne Sicherheitseinbuße zu reduzieren. Es wird vorgeschlagen, dass
- 15 der erste Teilnehmer (T1) von dem zweiten Teilnehmer (T2) eine Kennung (4) einholt und mit gespeicherten Kennungen (4) vergleicht. Bei übereinstimmender Kennung (4) ist ein dieser Kennung (4) zugeordnetes Sicherheitszertifikat (Cert) Basis für eine nachfolgende Datenübertragung und wenn keine übereinstimmende Kennung (4) vorliegt wird eine Sicherheitszertifikatsverifikation durchführt.
- 20

(Figur 1)

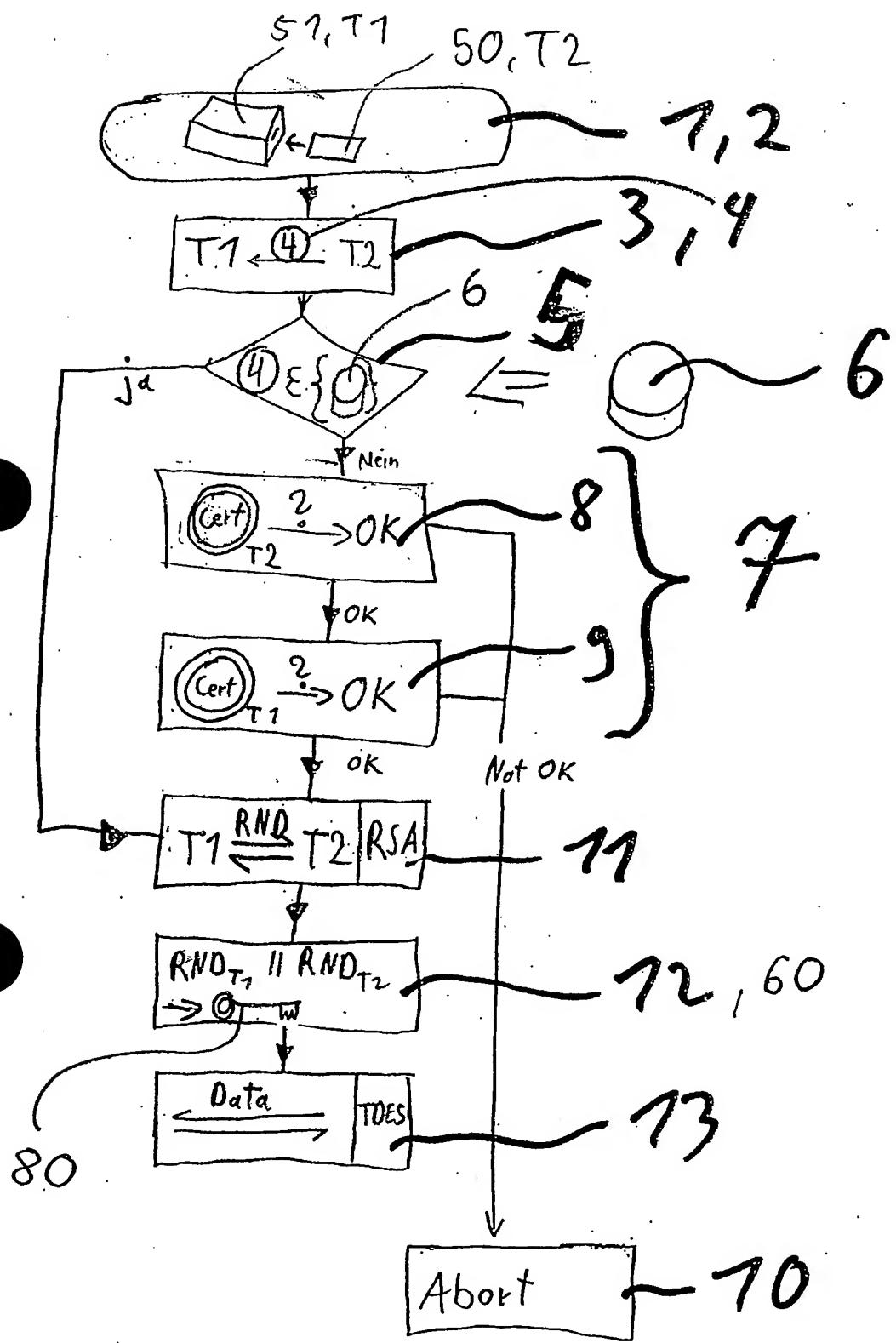


Fig. 1

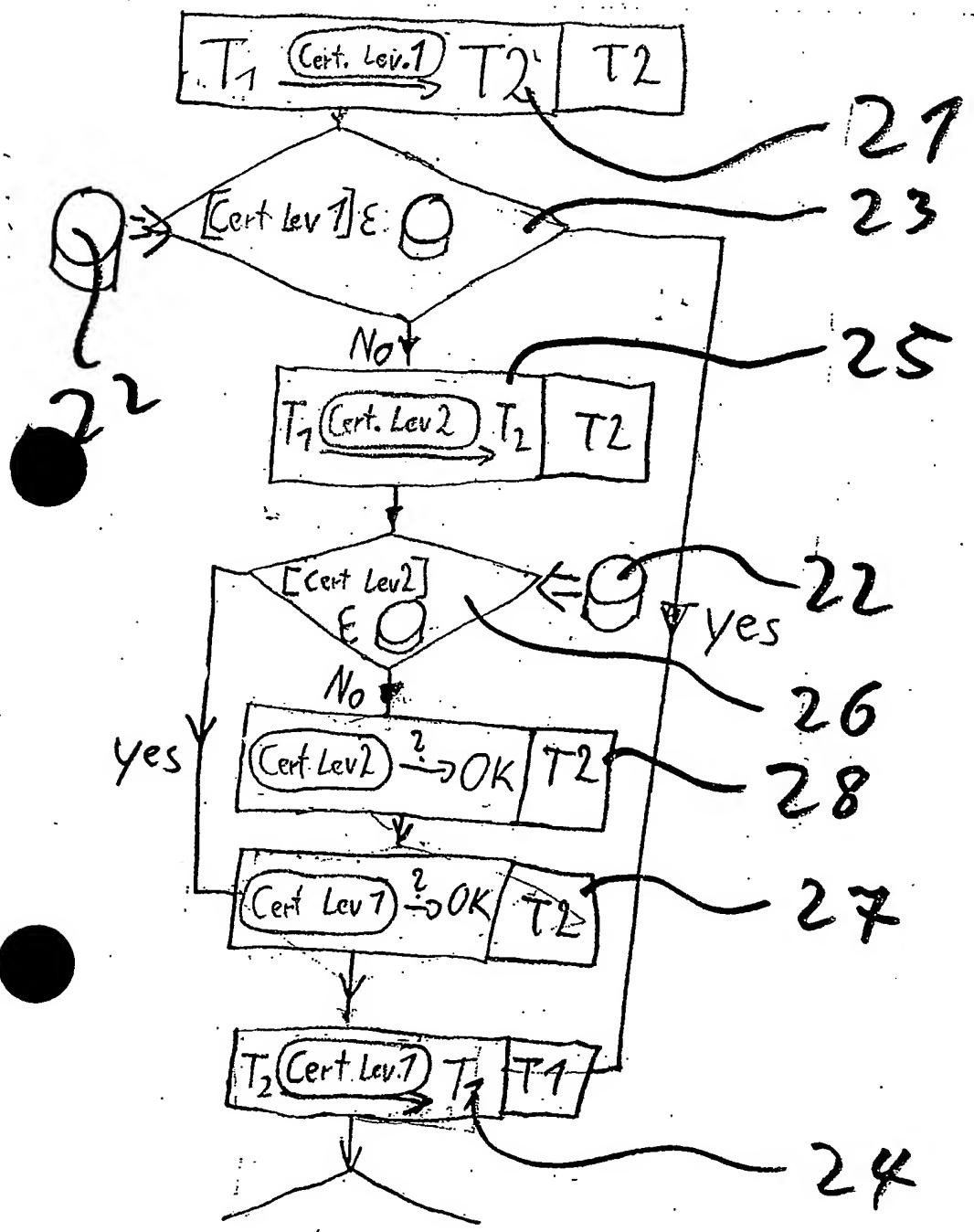


Fig: 2

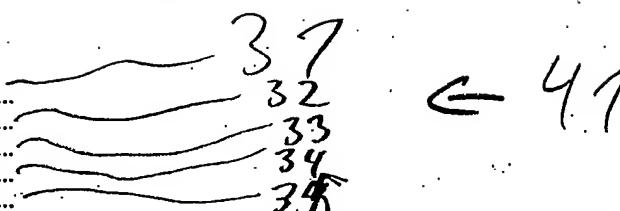
51

52

53
↓

Ausgangszustand Beispiel 5 Cardcontents:

Datum	CardContent (... EOF CHR ...)
0x00000000	... 0x00000000 0x0000000000000000 ...



Zustand nachdem 5 verschiedene Karten nacheinander gesteckt wurden:

Datum	CardContent (... EOF CHR ...)	(echtes Datum)
0x40346D00	... 0x43B71B7F 0x0000000000000001 ...	(19.02.2004 08:00:00) - 37
0x40347B10	... 0x43B71B7F 0x0000000000000002 ...	(19.02.2004 09:00:00) - 32
0x40348920	... 0x43B71B7F 0x0000000000000003 ...	(19.02.2004 10:00:00) - 33
0x40349730	... 0x43B71B7F 0x0000000000000004 ...	(19.02.2004 11:00:00) - 34
0x4034A540	... 0x43B71B7F 0x0000000000000005 ...	(19.02.2004 12:00:00) - 35

← 41

← 42

Zustand nachdem Karte 3 noch einmal gesteckt wurde am 19.02.2004 15:00:00

Datum	CardContent (... EOF CHR ...)	(echtes Datum)
0x40346D00	... 0x43B71B7F 0x0000000000000001 ...	(19.02.2004 08:00:00) - 37
0x40347B10	... 0x43B71B7F 0x0000000000000002 ...	(19.02.2004 09:00:00) - 32
0x4034CF70	... 0x43B71B7F 0x0000000000000003 ...	(19.02.2004 15:00:00) - 33
0x40349730	... 0x43B71B7F 0x0000000000000004 ...	(19.02.2004 11:00:00) - 34
0x4034A540	... 0x43B71B7F 0x0000000000000005 ...	(19.02.2004 12:00:00) - 35

← 43

36

Zustand nachdem Karte 6 gesteckt wurde am 19.02.2004 16:00:00

Datum	CardContent (... EOF CHR ...)	(echtes Datum)
0x4034DD80	... 0x43B71B7F 0x0000000000000006 ...	(19.02.2004 16:00:00) - 36
0x40347B10	... 0x43B71B7F 0x0000000000000002 ...	(19.02.2004 09:00:00) - 32
0x4034CF70	... 0x43B71B7F 0x0000000000000003 ...	(19.02.2004 15:00:00) - 33
0x40349730	... 0x43B71B7F 0x0000000000000004 ...	(19.02.2004 11:00:00) - 34
0x4034A540	... 0x43B71B7F 0x0000000000000005 ...	(19.02.2004 12:00:00) - 35

← 44

Zustand nachdem Karte 7 gesteckt wurde am 19.02.2004 17:00:00

Datum	CardContent (... EOF CHR ...)	(echtes Datum)
0x4034DD80	... 0x43B71B7F 0x0000000000000006 ...	(19.02.2004 16:00:00) - 36
0x4034EB90	... 0x43B71B7F 0x0000000000000007 ...	(19.02.2004 17:00:00) - 37
0x4034CF70	... 0x43B71B7F 0x0000000000000003 ...	(19.02.2004 15:00:00) - 33
0x40349730	... 0x43B71B7F 0x0000000000000004 ...	(19.02.2004 11:00:00) - 34
0x4034A540	... 0x43B71B7F 0x0000000000000005 ...	(19.02.2004 12:00:00) - 35

← 45

Zustand nachdem Karte 1 gesteckt wurde am 19.02.2004 18:00:00

Datum	CardContent (... EOF CHR ...)	(echtes Datum)
0x4034DD80	... 0x43B71B7F 0x0000000000000006 ...	(19.02.2004 16:00:00)
0x4034EB90	... 0x43B71B7F 0x0000000000000007 ...	(19.02.2004 17:00:00)
0x4034CF70	... 0x43B71B7F 0x0000000000000003 ...	(19.02.2004 15:00:00)
0x4034F9A0	... 0x43B71B7F 0x0000000000000001 ...	(19.02.2004 17:00:00)
0x4034A540	... 0x43B71B7F 0x0000000000000005 ...	(19.02.2004 12:00:00)

← 46

Fig. 3

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.